Secure Envelope and Email Data Loss Prevention

Demetrias Rodgers - Systems Integration Manager

July 11, 2012

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Technology Spotlight

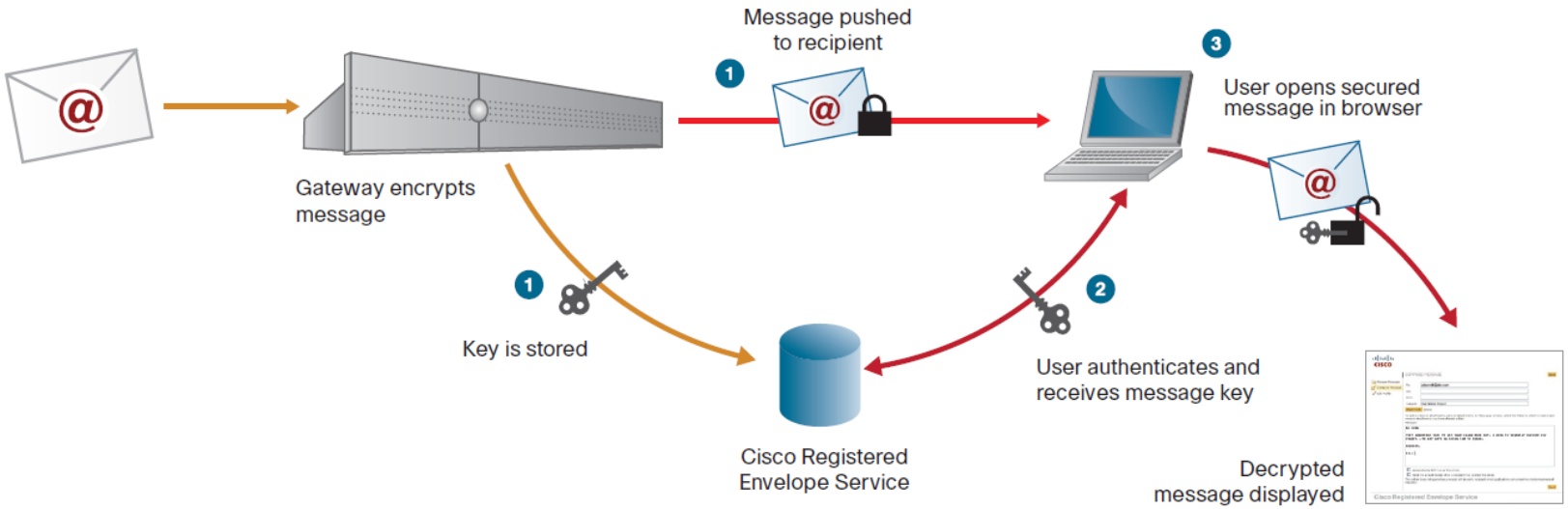
- Description:
  - We are looking to highlight various new technologies that will provide value to our customer agencies.
  - We are seeking feedback on these technologies to gauge interest in the introduction of these services into the service catalog.
  - Your feedback allows us to focus our resources on developing and introducing technology that you feel will bring the greatest value to the Commonwealth of Virginia.
  - The first sets of technologies we are here to highlight are secure envelope encryption capabilities and email data loss prevention.

Secure Envelope Encryption

- Secure envelope encryption allows for agencies to send encrypted communication to email users outside of the COV enterprise domain without requiring the outside entity to have public key infrastructure in place.
- Secure envelope encryption utilizes the existing IronPort appliances in place today and is an envelope-based "push" technology.
  - Encrypted messages can be received by any email user - independent of the email client, the operating system, or the device used - without the need to install any software or requiring the sender to pre-exchange encryption credentials.
- Secure envelope encryption satisfies encryption regulatory requirements without being a burden on the senders, recipients or email administrators. These requirements include:
  - Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX)

Secure Envelope Encryption

- Read receipts enable users to know exactly when a message was viewed by each recipient.
- Message expiration and recall prevents mistakenly sent messages from being opened and automatically secures old messages. The message may be recalled at any time, keeping the message from ever being opened again.

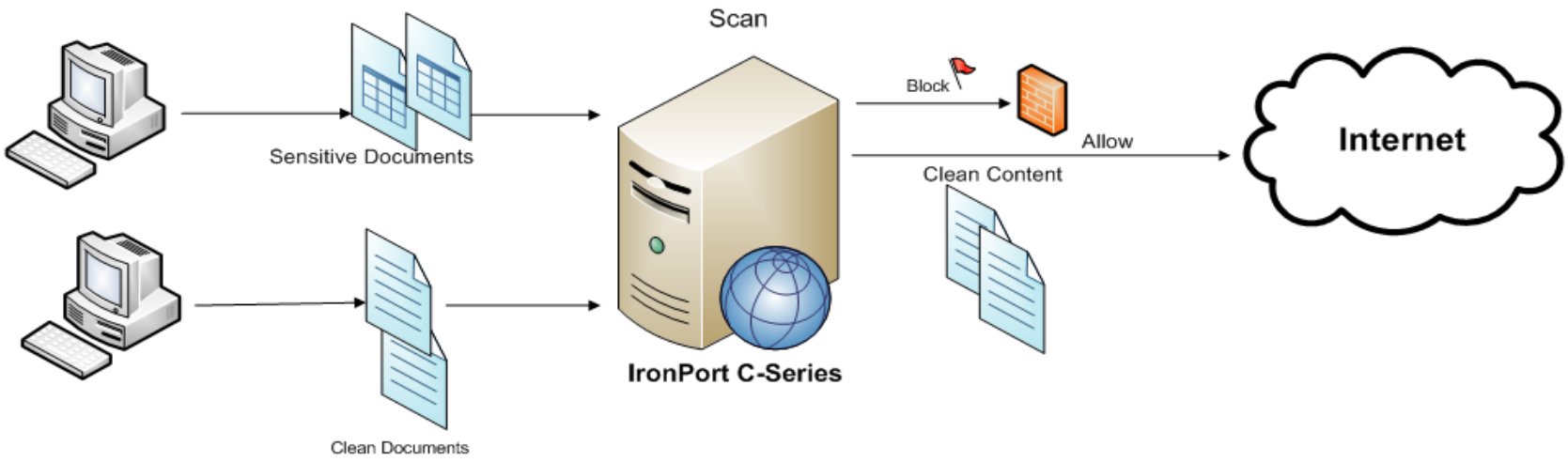


Email Data Loss Prevention

- Email data loss prevention (DLP) technology provides agencies the capability to perform content level scanning of email messages and attachments to detect inappropriate transport or sensitive information.
  - Examples: Credit card, Social Security numbers or corporate intellectual property
- Our enterprise email vendors have developed a DLP detection and enforcement engine that is a software featured that is licensed and becomes fully integrated into the IronPort appliance.
- Email DLP secures sensitive, health or personal data while it is being exchanged among different stakeholders, making sure that:
  - Data is scanned while in motion
  - Any potential flags are raised
  - Electronic or human mitigations are put into place if deemed necessary
  - Data is transmitted securely

Email Data Loss Prevention

- Pre-defined canned templates provide capability for compliance with regulatory legislation, such as HIPAA, SOX, Gramm-Leach-Bliley Act (GLBA), Personal Information Protection and Electronic Documents Act (PIPEDA).
- Customized DLP policies can be created if the existing predefined DLP policy templates are not sufficient. Polices are applied to the entire agency and not at the user level.
- If a sensitive message requires encryption, the message can be encrypted automatically using the secure envelope email encryption feature if subscribed.



Questions